FOURTH INTERNATIONAL SCIENTIFIC CONFERENCE: "CHALLENGES OF MODERN ECONOMY AND SOCIETY THROUGH THE PRISM OF GREEN ECONOMY AND SUSTAINABLE DEVELOPMENT" – CESGED2024

PROCEEDINGS

ISBN 978-86-82408-29-1

NOVI SAD, SEPTEMBER 2024.

PROCEEDINGS

FOURTH INTERNATIONAL SCIENTIFIC CONFERENCE:
"CHALLENGES OF MODERN ECONOMY
AND SOCIETY THROUGH THE PRISM OF GREEN ECONOMY
AND SUSTAINABLE DEVELOPMENT"- CESGED 2024
NOVI SAD, 19-22 SEPTEMBER 2024

ISBN 978-86-82408-29-1

PUBLISHERS:

- **FACULTY OF ECONOMICS AND ENGINEERING MANAGEMENT – FIMEK, NOVI SAD, SERBIA;**
- **EDUCATIONAL AND BUSINESS CENTER FOR DEVELOPMENT OF HUMAN RESOURCES, MANAGEMENT AND SUSTAINABLE DEVELOPMENT, NOVI SAD, SERBIA;**

INTERNATIONAL SCIENTIFIC BOARD

Branko Štrbac, PhD, associate professor (Serbia)
Boris Radovanov, PhD, associate professor (Serbia)
Sanja Dobričanin, PhD, associate professor (Serbia)
Tamara Premović, PhD, associate professor (Serbia)
Maja Dimić, PhD, associate professor (Serbia)
Jelena Lukić Nikolić, PhD, associate professor (Serbia)
Adrijana Maksimović, PhD, assistant professor (Serbia)
Adem Preljević, PhD, assistant professor (Serbia)
Elvis H. Mahmutović, PhD, assistant professor (Serbia)
Marko Pavlović, PhD, professor (Serbia)
Željko Račić, PhD, professor (Serbia)
Darko Marjanović, PhD, senior research associate (Serbia)

INTERNATIONAL ORGANIZING COMMITTEE

Branislav Dudić, PhD, associate professor (Slovakia)
Jelena Premović, PhD, senior scientific associate (Serbia)
Aleksandar Ašonja, PhD, full professor (Serbia)
Zana Dolićanin, PhD, full professor (Serbia)
Edin Dolićanin, PhD, full professor (Serbia)
Leila Gholami, PhD, associate professor (Iran)
Sabri El Mouatassime, PhD, assistant professor (Morocco)
Velibor Spalević, PhD, associate professor (Montenegro)
Goran Škatarić, PhD, associate professor (Montenegro)
Aleksandar Brčić, PhD, assistant professor (Republic of Srpska)
Tamara Premović, PhD, associate professor (Serbia)
Milan Ivkov, PhD, associate professor (Serbia)
Borislav Savković, PhD, associate professor (Serbia)
Branko Štrbac, PhD, associate professor (Serbia)
Lazar Stošić, PhD, associate professor (Serbia)
Sanja Škorić, PhD, associate professor (Serbia)
Nenad Bingulac, PhD, associate professor (Serbia)
Dejan Logarušić, PhD, associate professor (Serbia)
Dalibor Krstinić, PhD, associate professor (Serbia)
Vladimir Šipovac, PhD, associate professor (Serbia)
Jelena Lukić Nikolić, PhD, associate professor (Serbia)
Tibor Fazekaš, PhD, assistant professor (Serbia)
Jovana Gardašević, PhD, assistant professor (Serbia)
Violeta Milićević, PhD, professor (Serbia)

Marko Gašić, PhD, professor (Serbia)
Marija Perić, PhD, professor (Serbia)
Zoran Papović, PhD, professor (Serbia)
Nataša Lukić, professor (Serbia)
Vladimir Mirković (Serbia)
Dejan Zejak (Montenegro)
Aleksandra Perić, MSc (Serbia)
Marko Drašković, MSc (Serbia)
Tamara Krstić (Serbia)
Vladimir Pejanović (Serbia)
Minja Tanasković (Serbia)
Andrej Andrašik (Serbia)

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад

330.34:502(082)
502.131.1(082)

INTERNATIONAL Scientific Conference "Challenges of Modern Economy and Society through the Prism of Green Economy and Sustainable Development" – CESGED 2024 (4 ; 2024 ; Novi Sad)
Proceedings [Elektronski izvor] / Fourth International Scientific Conference "Challenges of Modern Economy and Society through the Prism of Green Economy and Sustainable Development" – CESGED 2024, Novi Sad, 19-22 September 2024 ; [editors Branislav Dudić, Jelena Premović]. - Novi Sad : Faculty of Economics and Engineering Management – FIMEK : Educational and Business Center for Development of Human Resources, Management and Sustainable Development, 2024

Način pristupa (URL): https://www.cesged.com. - Opis zasnovan na stanju na dan 20.12.2024. - Bibliografija uz svaki rad.

ISBN 978-86-82408-29-1

а) Економија -- Еколошки аспект -- Зборници б) Одрживи развој -- Зборници

COBISS.SR-ID 159727881

INTERNATIONAL SCIENTIFIC CONFERENCE:
"CHALLENGES OF MODERN ECONOMY AND SOCIETY THROUGH THE PRISM OF GREEN ECONOMY AND SUSTAINABLE DEVELOPMENT" – CESGED2024
Novi Sad (Serbia), 19-22 September 2024.

Organizers of the conference:

• EDUCATIONAL AND BUSINESS CENTER FOR DEVELOPMENT OF HUMAN RESOURCES, MANAGEMENT AND SUSTAINABLE DEVELOPMENT, NOVI SAD, SERBIA;

• COMENIUS UNIVERSITY BRATISLAVA, FACULTY OF MANAGEMENT, BRATISLAVA, SLOVAKIA;

• EDUCATIONAL CENTER FOR TRAINING IN PROFESSIONAL AND WORK SKILLS, NOVI SAD, SERBIA;

• UNIVERSITY OF ECONOMIC ACADEMY IN NOVI SAD

- FACULTY OF ECONOMICS AND ENGINEERING MANAGEMENT – FIMEK, NOVI SAD, SERBIA
- FACULTY OF LAW FOR COMMERCE AND JUDICIARY NOVI SAD, SERBIA

• STATE UNIVERSITY OF NOVI PAZAR, NOVI PAZAR, SERBIA;

• BIOTECHNICAL CENTER, BIJELO POLJE, MONTENEGRO

Time and place of the conference:

• NOVI SAD, *19.09-22.09.2024.*

Educational center for training in professional and work skills - conference hall,

Novi Sad, Industrijska no. 3;

Thematic areas:

• Green economy and sustainable development;
• Multidisciplinary approach in research:
  - economic sciences;
  - legal sciences;
  - mathematical sciences;
  - technical and technological sciences;
  - biomedical sciences;
  - philological sciences;
  - philosophical sciences and art;
• Economic theory and politics;
• General economy and economic development;
• Business and International Economics and Management;
• Entrepreneurship, leadership and human resource management;
• Management in service activities:
  - tourism and hotel industry;
  - healthcare;
  - agriculture and agribusiness;
  - education and sports;
  - culture and public information;
  - public sector and state administration;
  - banking and finance;
  - traffic;
  - construction; etc.
• Marketing, trade and logistics;
• Accounting, auditing and business finance;
• Business informatics and quantitative methods;
• Investments and technical-technological development;
• Industry 4.0;
• Law, security and criminology;
• Demographics and sociological-psychological research;

PERSONAL DATA PROTECTION IN EMPLOYMENT LAW

Dejan Logarušić[1], Denis Tul[2], Jovan Vlaški[3]

[1]University of Business Academy, Faculty of Law for Commerce and Judiciary in Novi Sad, Serbia,
email: dejan.logarusic@pravni-fakultet.info
[2]University of Business Academy, Faculty of Law for Commerce and Judiciary in Novi Sad, Serbia,
email: denis.tul@pravni-fakultet.info
[3]Master of Law, Faculty of Law in Kragujevac, Serbia

ABSTRACT:

The field of employment law is largely intertwined with the protection of personal data, given that a large amount of personal data is processed within the process of candidate selection and employment. The Employment Law of the Republic of Serbia is not fully harmonized with the Legal Act on Personal Data Protection, and the relationship between these two laws is very important for the aforementioned issues. All companies have databases of job candidates and employees. In the first case, these are only persons who can potentially conclude a contract with the employer, but in the second phase, it is the base of employees who already have employment contracts with the employer. With extensive databases, come the issues of protection and storage of personal data of job candidates and employees of the employer. Employment law is faced with new challenges. One of those challenges is establishing best practices, and creatively solving practical issues related to the processing of personal data.

Keywords: *Personal data, Protection of personal data, Employment law, Employees, IT Law.*

1. INTRODUCTION

The protection of personal data is rapidly evolving, not only due to the swift changes in regulations but also because of the rapid development of technologies and technological advancements. At the intersection of information technology law and personal data protection law, new questions are emerging across every legal area, including traditional areas such as employment law.

Changes in the modern world cannot leave employment law untouched. "The Fourth Industrial Revolution represents a technological revolution. With the development and arrival of new technologies, we are witnessing changes in the way humanity lives. Technology influences how we perceive ourselves and affects human identity. These core and fundamental changes brought about by new interactive technologies represent the essence of the Fourth Industrial Revolution. This primarily refers to 5G internet, fast transmission of vast amounts of data, numerous databases, blockchain technology, artificial intelligence, and others [6]."

It is the duty of legal professionals and the legal field to monitor these changes and respond appropriately to ensure that companies operate smoothly and apply new legal provisions in a purposeful and correct manner. All trends in modern business must be accompanied by a legal perspective.

Personal data protection law is based on two key documents: at the European Union level, the General Data Protection Regulation (GDPR) [14], while in Serbia there is the new Legal Act on Personal Data Protection (LPDP) in force since 2019. This legal act has brought revolutionary changes in the field of personal data protection.

All companies today strive for automation of processes, which involves the use of technology in many areas of business. Nowadays, companies process data electronically, collect data electronically, store data in electronic databases, and data transmission, as a separate issue, is also digitized. Since companies aim to maintain an online presence and conduct marketing via social networks, it is clear that IT law requires our attention. It is indisputable that one of the most important parts of IT law is, in fact, personal data protection law. Therefore, we must start with Professor Savin Andrej's assertion: "Privacy is the ability of an individual to keep

information about themselves secret, or in other words, to keep part of their life private and choose which aspects to make public [1].”

Given the above, science cannot keep pace with the changes we see in practice, but every scientific work in these fields, especially one focused on solving practical problems, is of great significance. This is where we see both scientific and societal benefit, given that all these topics impact society as a whole, as employment law and the position of employees concern all of us.

The methods used in the preparation of this paper are standard methods in the field of social sciences, particularly legal science. This primarily refers to the analysis of legal provisions and the interpretation of legal acts, combined with appropriate modern methods.

2. PERSONAL DANA PROTECTION AND EMPLOYMENT LAW

The question of personal data protection in the field of labor law is addressed by three laws simultaneously. Primarily, the LPDP, as a law that governs all types of data processing, and secondly, the Legal Act on Employment Law. The Employment Law provides a foundation and does not contradict the LPDP, but it does not provide sufficient guidance on how data is processed and how personal data is managed. Therefore, the law we will refer to most is the LPDP, as the act that regulates the process of personal data processing in the most detail. In addition to these two legal acts, there is also the Legal Act on Records in the Field of Labor, which determines which records are mandatory, which does not exclude the employer's right to keep other records not explicitly mentioned here.

The Legal Act on Employment Law has not been amended since the adoption of the new LPDP, and therefore it is not aligned with the changes introduced by the LPDP. Article 83 of the Legal Act on Employment Law, "protection of personal data", deals with the protection of personal data. We quote the mentioned article for analysis:

"Employees have the right to view documents containing personal data held by the employer and the right to request the deletion of data that is not directly relevant to the work they perform, as well as the correction of inaccurate data.

Personal data relating to an employee may not be made available to a third party, except in cases and under conditions provided by law or if it is necessary to prove rights and obligations arising from the employment relationship or in connection with work.

Personal data of employees may only be collected, processed, used and provided to third parties by an employee authorized by the director [8].“

The LPDP, in Article 91, briefly states that this should be regulated by employment law provisions [9]. This is insufficient, and ambiguities can arise regarding the application of these provisions. Interpreting the legal provisions governing the field of employment law, we encounter a major problem regarding the protection of personal data, and that is that the Legal Act on Records in the Field of Labor is still in force, which is outdated and almost inapplicable, partly due to the development of technology. The employer has an obligation to ensure the protection of data and its confidentiality for its employees, while employees are obliged to care for and ensure the protection of personal data (of other employees, clients, and third parties) to which they have access in performing their work tasks. Employees must be informed about how and in what way their personal data is processed. Also, one of the important obligations of the employer is to inform and educate employees about the consequences of violating the right to privacy of personal data of other persons [5].

In the field of employment law, there is also the Legal Act on Records in the Field of Labor (1997) (hereinafter: LRFL). This law was adopted some time ago and is not aligned with the LPDP, which poses an additional challenge for employers. LRFL lists some of the records kept by the employer, including: a record of employees, a record of vacant positions, a record of unemployed persons, a record of employee salaries, records of offers from foreign employers for the employment of our citizens abroad, a record of our citizens working abroad, a record of unemployed foreign citizens or stateless persons in our country, and a record of beneficiaries of disability insurance benefits [10]. In addition to the listed records, the employer may keep many other records that serve in its business, with different purposes and legal bases for different records.

Employees, in the context of personal data processing, are viewed from two perspectives: as individuals whose data is processed (which is the focus of this paper) and as individuals who, within the employer and employer's procedures, participate in data processing. Thus, Professor Đorđe Krivokapić [3], and his associates say: "Employees have a duty to

comply with the employer's instructions, internal procedures, and the broader legal framework in the course of their work. While the relationship between employees and employers should be based on mutual trust, violation of data protection laws by employees can lead to the employer incurring financial, operational, regulatory, reputational, and other costs."

3. DATABASES AND EMPLOYMENT LAW

Databases are collections of data or data sets, as explicitly stated by the LPDP. A database is any structured set of data sorted according to specific criteria.

Databases can be centralized or decentralized. A decentralized database means that it is located in multiple places (parts of the database).

There are two types of databases that occur with controllers or processors and that are significant from the perspective of employment law:

1. Employee database (employee files);
2. Job candidate database (hiring process).

This division is made according to the individuals whose data is being processed. Each of these databases implies a different scope of data, a different purpose and legal basis for collection, and different rules of procedure and retention periods for this data.

3.1. Employment database

In addition to the LPDP, the Employment Law also deals with the protection of personal data of employees, specifying which data can be collected for the purpose of concluding an employment contract. For this reason, this is a slightly more complex issue, and care must be taken to apply both laws, which are not contradictory but, as we can see, the Employment Law supplements the LPDP in some ways. The protection of personal data is regulated within the framework of the protection of the rights of employees, while in some scientific works it can be seen as a part of safety and health in a workplace [7].

Confidential data significant from the standpoint of work and employment can be divided into three groups - information about employees, management, and business information [17].

When entering into an employment relationship, the employee must provide certain personal data, which puts the employer in a subordinate position. The employer has an obligation to keep records of employees in order to enable the smooth operation of the business or the realization of the employees' labor and social rights. The Legal Act on Employment Law itself hardly regulates the issue of personal data protection; it can be said that it is poor in the part where it regulates the employee's right to data protection [4].

"The purpose of these databases is for the employer to ensure, on the one hand, security, and on the other, the realization of the employees' labor rights. Logically, the employer must have the bank account of their employees in order to be able to pay them their salaries. This is, first and foremost, in the interest of the employees who receive salaries. This is a trivial example, but the logic behind these databases is clear [2]."

Some countries adopt special laws that regulate information about employees that falls within the domain of confidentiality and refers to data on the basis of which it is possible to identify the employee or job candidate [5].

If an employee, in performing their job duties, comes across personal data and, without the knowledge of the employer, i.e. the data controller, transfers it to a third party, they can be found guilty of a serious violation of their work obligations, which is enforced in disciplinary proceedings [16]. The Legal Act on Employment Law does not contain in its provisions a sanction for an employee who has violated the right to the confidentiality of user data. If it concerns particularly sensitive data of third parties, it is not enough for the processor to have the consent of the data controller, but the consent of the person whose data is being processed is also required. The European Union supports this view when it comes to assessing the potential liability and protection of personal data in the field of work and employment.

It is common for some employers to temporarily engage persons through employment agencies. The fact that the employer is in this sense a user in a three-way relationship. It is not an obstacle to use and process the data of a person who is temporarily employed with them. The employer can create a separate database for such persons and process the personal data

that is necessary for them. The employer-user assumes the responsibility for processing personal data with all the obligations and responsibilities that it also has towards its employees. The agency that has provided these employees to the employer must create separate records and process the data on the basis of which it will carry out its activities.

If the declaration for mandatory social and health insurance and the payment of remuneration for work is carried out by the agency of intermediaries, the employer with whom the work is performed is not obligated and it is considered excessive processing of data such as the current account, health record number, and LBO from the health record, if it is not really necessary for the fulfillment of other legal obligations. The Legal Act on Employment Law is not applicable to non-classical forms of work, i.e., the protection of personal data according to the Employment Law does not apply to persons who are not in an employment relationship but, for example, are employed under a contract for work or a contract for temporary and occasional work. Since the LPDP does not distinguish between categories of employees according to these persons, rights and obligations will be same as they were employees. The obligation towards members of cooperatives who are engaged in temporary and occasional work in accordance with a special law [13], will be borne by the cooperative, as well as by the employer to whom the member is sent to work.

Of course, the protection of personal data in the field of Employment Law is important to reduce excessive interference by the employer in the employee's private life. It is necessary to more closely regulate by law the conditions for disclosing personal data in the field of work and employment in order to reduce and prevent negative consequences for employees, ensure the protection of the interests of employers, and protect the privacy of employees.

3.2. Job candidate databases

The employer comes into possession of certain personal data even before the employment contract is concluded, i.e., before establishing an employment relationship between them and the person whose data they process as a potential job candidate. Job candidates often submit their CVs (Curriculum Vitae) to potential employers before entering into an employment relationship, which contains a range of personal data. By applying and sending their CV to the employer, the job candidate may give

their consent to the processing of data by a conclusive act, by the very act of submitting their CV. Of course, the employer must process the data unambiguously only in relation to the application for the given position, and it must not be excessive in relation to the purpose for which it is processed. Many job boards and companies themselves, when posting a vacancy for a particular job, request the candidate's consent to process personal data.

Employers can collect and process data from potential job candidates that relates exclusively to the candidate's qualifications and expertise for the position they are applying for. Excessive processing would be considered if the employer requires knowing your residential address or personal ID [12]. Namely, the employer can ask their candidate to tell them the place where they live if it is necessary for them, for example, to calculate the amount of travel expenses and other earnings, but not the exact residential address [11], which, for example, includes the street and house number. The same applies to requesting a personal ID, which is considered purposeless in the initial phase of applying for a job, i.e., before concluding an employment contract. The employer may require special conditions that interfere with personal data, but they must be closely related to the job that the person will perform. Special conditions are those found in the job description and classification or described in the employment contract. For example, educational qualifications, the educational institution that the candidate attended, the overall grade point average achieved. Of course, there are also special conditions that apply to the employment of certain categories, which require the employer to collect more personal data than the usual procedure. For example, if a person with a disability is employed, the employer must collect information about the remaining work capacity.

"According to the logic of the LPDP, the employer should only collect data on professional qualifications and experience, but not data on the residential address, personal ID, and other data that is not crucial for making a decision on employment. However, in practice, everyone can put any data they want in their CV, and this is often done without thinking about protecting their own personal data [2].

There are certain questions that employers should definitely avoid asking during job interviews, even though many do ask them, thereby infringing on the privacy of job candidates. Examples include: marital status, family planning, and whether the candidate owns their own home, i.e., their material and financial status. Of course, there may be some exceptions if this is necessary for the performance of the job. For example, if the

employer requires the employee to have their own vehicle, they can ask about the vehicle and possession of a driver's license.

Many employers, when posting job advertisements, indicate that the CV should include a photo of the potential candidate. The question arises as to the reason for collecting and processing this type of personal data. Can this be considered excessive processing, i.e., does the employer really need to have a photo of the job candidate at that stage? Based on the photo alone, the employer can obtain and collect a lot of sensitive personal data, such as religious affiliation, race, gender, and health condition. Based on the photo that the employer receives in the CV, discrimination in the selection of candidates may occur. Therefore, I believe that requesting a photo in the first phase of applying for a job is excessive processing of personal data.

4. SECURITY OF THE DATABASE AND SECURITY OF PERSONAL DATA

Employers are obligated to collect employee data in compliance with legal provisions, but also to protect these databases in accordance with specific legal requirements.

One of the fundamental principles of data processing is the principle of confidentiality and integrity, as stipulated in Article 5(1)(f) of the LPDP. This principle states that the controller (in this case, the employer) must process personal data in a manner that ensures an appropriate level of security of personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

How do employers implement this principle? The answer lies in the process of aligning business operations with the LPDP.

This process aims to ensure that the controller or processor aligns all elements and phases of their operations with the LPDP. This involves preparing documentation and implementing measures.

Documentation comes first and outlines how the controller will proceed in this process, i.e., what the data processing process will look like, whether digital data processing is possible and how it is carried out, what data is processed, how and for how long it is stored, and so on.

The law categorizes measures into three categories:

- Technical;
- Organizational;
- Personnel.

Technical measures relate to the technical aids and tools used by the employer and their impact on data. How data is entered, who enters it, how it is stored, and where. For example, where data is stored is very important. In practice, company data is much more secure when stored on their own servers, rather than on servers rented from third parties. These third-party servers can be, and often are, located abroad, which also constitutes data export. Of course, data on the internet is not as secure as data stored on servers that are not connected to the internet. Such data can only be compromised physically, by destroying the server or accessing it and transferring the data to a USB drive. However, such servers are stored in locked rooms, which brings us to the second category of measures.

Organizational measures relate to how the employer has organized their activities, what the work processes look like, who can potentially compromise the data, and at what stage of the business. Of course, there must be certain barriers in place to prevent data misuse.

Personnel measures relate to the number of people at the employer who have access to personal data in their work. Of course, the fewer people who have access to data, the less likely it is that someone will misuse that data. Therefore, if it is possible to establish some part of the business in such a way that fewer people have access to data, this should be done.

Therefore, the employer, as a controller or processor of personal data, is obliged to implement all possible measures to minimize the risk to personal data.

In the absence of domestic practice under the LPDP, we would highlight one practical example from the environment, from Romania, where the GDPR is in force. Namely, the company Bristol Logistic had an incident where an employee stole the files of twelve (12) workers. According to the GDPR, this company was fined 2,000 euros [18]. Namely, the example suggests that it is the employee's fault, and that he should be held responsible for his actions, and that is true, but here there is also the fault of the company that did not secure the files sufficiently and thereby enabled the employee to misappropriate them. According to the area of personal data protection, the company was obliged to implement technical,

organizational, and personnel measures to secure personal data. Since they were located on a shelf, unlocked, the competent authorities concluded that the employer himself was also guilty, and was fined in accordance with the provisions of the GDPR.

Therefore, databases of employees and job candidates, by the employer who acts as a controller here, must be protected. Access to these databases should not be allowed to a wider circle of employees. This implies a much broader consideration. For example, is it possible to throw away a printed CV of a job candidate in the trash after the end of a competition in which they were not employed? It shouldn't. If, after the shift, the cleaners were to clean the premises, is it realistically possible for them to take a crumpled CV, open it and further manipulate the personal data at their own discretion? Yes, therefore, we must implement measures to protect personal data.

5. PRACTICAL ISSUES

Now that we've examined the types of databases that are important to employers in employment law and have discussed how to securely manage these databases in the following chapter, the question arises: "What is actually happening in practice in this area?" In this chapter, we will explore specific issues that have arisen in employment law and in the relationship between the employer as data controller and the employee as the data subject.

It must be noted that the practice in Serbia is not yet rich with processed cases, either by the Commissioner or by the competent courts. We have the impression that the application of the LPDP is late. Practical examples come from the practice of the Commissioner and the practices of economic entities themselves, who are aligning their operations with the legislative framework.

5.1. Records of time spent at work (arrival/departure)

Since the inception of organized work, there have been records of working hours, i.e., the time an employee has spent at work. Over the years, and with the advent of new technologies, the methods of keeping these records have changed. Previously, employees would manually record their arrival

time on a piece of paper or in a notebook. With the advent of computers, this record-keeping began to be executed electronically.

Some employers sought to control employee arrival and departure by scanning their fingerprints upon entering and exiting the company premises. The collection of fingerprint images and the use of fingerprint algorithms for time and attendance records represent a disproportionate processing of personal data in terms of Article 8 (7) of the LPDP. The processing of personal data, including fingerprint images converted into algorithms, is not permitted if there is no adequate legal basis for such processing.

The "Dr. Dragiša Mišović" Health Center, headquartered in Čačak, Serbia, installed such an employee attendance system [19]. Following a complaint, the data protection commissioner conducted an inspection and issued a warning [15]. In this case, even if the employer had obtained the consent of all employees for the collection and processing of this data and had implemented all necessary safeguards, this type of record-keeping would have been excessive. Before implementing the system, an assessment should have been conducted to determine whether employee arrival and departure could be controlled by other means without collecting sensitive personal data. The same would apply if they had introduced a device that photographed the face of the person checking in at a given moment. Access control using "touch" systems is perhaps the most data protection-friendly method of controlling the fulfillment of work obligations. "Touch" systems typically only process the employee's name, surname, and the organizational unit to which they belong. Along with the time of entry and exit, this represents a minimal amount of personal data processing for this purpose. Manual entry in a logbook is similar to the "touch" system, but it is considered more susceptible to abuse, as any user can check when someone entered and whether a particular employee has arrived at work. With "touch" systems, access to records is restricted to authorized personnel.

5.2. Supervision of employees working from home

Initially, modern trends introduced a new type of work: remote work, or working outside the employer's premises. The COVID-19 pandemic significantly accelerated this process, making the benefits of remote work more apparent to businesses and employees alike. This rapid adaptation to new work arrangements raised numerous questions that society had not

previously addressed. While some companies retained remote work post-pandemic, others adopted a hybrid model combining on-site and remote work.

In the preceding sections, we discussed employees and their personal data. Here, employee data takes on a new dimension, aligning with the aforementioned issues.

With the rise of remote work, the element of employer oversight has diminished. To ensure that employees are contributing the required work quality and quantity, employers must implement some form of monitoring.

Various creative solutions have emerged to protect the employer's interests. However, these measures often infringe on the privacy of remote workers. Techniques such as tracking keystrokes and taking random screenshots have been employed but are considered violations of privacy and data protection laws, especially when personal devices are involved.

Imagine a personal notification popping up on your screen. If a monitoring application were to capture a screenshot at that moment, it could expose your private messages. This would constitute a significant invasion of privacy.

Experts agree that monitoring tools should minimize the risk to personal data and privacy while still achieving the desired results. If a goal can be accomplished with less intrusive data collection, that method should be preferred. Many applications have been found to involve excessive processing of personal data.

This issue is complex and evolving. Solutions must be developed at the intersection of IT and law. One approach is task-based management, where employees are assigned tasks with estimated completion times. Employers evaluate the quality of the work without tracking time spent. While this method has its pros and cons, it is effective in protecting personal data as it does not require the employer to collect detailed employee information. The employer simply needs to verify that the task has been completed on time.

5.3. Tracking the location of employees in the field

Another form of employee data processing is tracking the location of an employee working in the field. This can be seen with employers engaged in the transportation of people and goods (e.g., transport, taxi services, etc.)

and with companies involved in deliveries (e.g., by car, motorcycle, bicycle, etc.).

Some of these companies use applications that track the location of the employee. When the employee starts their work shift, they activate the application and appear on the map of active employees, and the company can monitor the map showing the locations of all employees who are logged in. There are also more extreme situations where locators are used, and employees cannot turn them off even after they finish their work hours.

Many employers install GPS devices in their vehicles to track their movement. The employer generally justifies the installation of the GPS device with the legitimate interest of protecting their property and controlling work-related costs (e.g., fuel consumption). The employer is obligated to obtain the employee's consent for data processing. Naturally, the problem of legitimate interest arises when the employer provides the vehicle to the employee for 24-hour use, meaning the vehicle can be used for personal purposes. If the vehicle is used by the employee outside of working hours, the employer should not, in principle, analyze or misuse the employee's location data outside of work hours, as this encroaches on privacy. This raises the question: Does this exceed the legitimate interest of protecting property?

5.4. Video surveillance of the workplace

In certain situations, the employer may wish to monitor the employee during work at the workplace. This is a sensitive issue, and the official stance is that this is not allowed. The explanation is clear and is based on the principle of data minimization, as well as the employees' rights to privacy.

However, in some situations, this can be implemented, and such processing can be considered lawful. One of the most common justifications encountered in practice is the protection of high-value assets and persons. Sometimes this can be a valid reason for installing cameras. It is a matter of assessing each specific situation.

The installation of video surveillance is a right of the property owner, but in such cases, the purpose of the video surveillance is to ensure the safety of persons or property, and as such, it cannot be installed in a way that violates the employee’s right to privacy. In cases where data obtained through video surveillance is processed, the primary basis may be

considered a legitimate interest. Legitimate interest must be real and current, meaning that without video surveillance, significant damage or danger to property could occur. The Legal Act on Private Security prescribes the manner and duration of data retention obtained in this way [10].

If the employer installs video surveillance due to legitimate interests, they are obligated to obtain consent from their employees for the processing of data obtained through the surveillance. If video surveillance is used to monitor arrivals and departures from work, the employer must first conduct an analysis to determine whether this monitoring can be conducted in another way, using a smaller amount of personal data processing. Often, there will not be a legitimate interest that can justify such monitoring.

6. CONCLUSION

The protection of personal data underwent a revolution in 2019 with the adoption of the new Legal Act on Personal Data Protection (LPDP). At the time of writing this paper, the law was still not being fully implemented. Nevertheless, we have encountered many practical issues that have forced us to discuss these matters at a higher level.

One of the areas significantly impacted by the regulatory changes is undoubtedly employment law. The employer, as a legal entity, always processes the personal data of its employees, as well as job candidates.

The aim of the Legal Act on Personal Data Protection (LPDP) (and also GDPR) is not to prohibit the processing of personal data, but to provide clear guidelines on how this processing should be carried out to minimize the risk of personal data breaches.

Data protection is important for employers as data controllers and for employees as data subjects. This adds another layer to the employer-employee relationship, where the employer has certain obligations, primarily to protect the privacy of the employee by safeguarding their data. It is unrealistic for the employer not to collect employee data. In the end, it is in the employees' interest to provide their data in order to exercise their legal rights. Some data are provided during the process of establishing an employment relationship and signing an employment contract, while other data are processed during the course of the employment relationship (such as medical data needed to open sick leave or maternity leave).

This function of the employer, as the data controller responsible for protecting employee privacy and data, is carried out through the application of various technical, organizational, and personnel measures. Employee files must be specially protected with appropriate measures. These measures will vary depending on whether the data is stored in electronic or physical form.

The databases must be created and further utilized in accordance with legal principles. However, due to the specific nature of the field, many complex issues arise in this area of law. Timekeeping records, which represent part of employee performance control, are a tool at the employer's disposal. Employee monitoring during remote work and fieldwork are also controversial issues. In any case, the principle of data minimization must always be kept in mind, meaning that only the minimum necessary data should be processed to achieve the purpose. For example, if monitoring a remote worker involved constant camera surveillance in the worker's private home, household, and family life, it would represent an extensive interpretation of data processing in relation to its purpose. If there is even one way to provide the employer with the necessary information about the employee's job performance with less data, it should be done in that way with minimal data processing.

Data processing in employment law cannot be avoided, but it can be arranged in such a way that it does not negatively impact employee privacy. We should handle the data of others in the same way we would want our data to be handled.

7. REFERENCES:

[1] Savin, A. (2020.). Digital rights - Legal regulation of the Internet in the European Union. Clio.

[2] Tul, D. Mitić, T. (2023). Personal data protection (manual). KEC grupa, Нови Сад.

[3] Krivokapić, Đ. Adamović, J. (2023). Personal data protection in business. Faculty of Organizational Sciences, Belgrade.

[4] Reljanović M.. Protection of personal data in Serbia - collection of papers. Belgrade.

[5] Stojković–Zlatanović, S. Lazarevic, B. (2017). Confidentiality of

personal data, implications for the position of employees from the point of view of judicial practice.

[6] Milojević, G. Tul, D. (2023). The concept and nature of digital assets. In: "Law days - Prof. Dr. Slavko Carić" - Two decades of development of legal thought (ed. PhD Milan Počuča): number of pages from 152 to 163. University of Business Academy in Novi Sad, Faculty of Law for Economy and Justice in Novi Sad. Novi Sad. УКД: 347.23:004.78. ИСБН: 978-86-86121-58-5.

[7] Mirjanić, Ž. (2019). Protection of personal data of employees in terms of the use of information technologies. Proceedings of the Faculty of Law in Niš, number 85. Niš.

[8] Labor Law (Official Gazette of RS No. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - US decision, 113/2017 and 95/2018 - authentic interpretation).

[9] Legal Act on Protection of Personal Data ("Official Gazette of RS" No. 87/2018).

[10] Legal Act on Private Security (Official Gazette of RS, No. 104/2013, 42/2015 and 87/2018).

[11] Legal Act on Residence and Residence of Citizens (Official Gazette of RS, No. 87/2011).

[12] Legal Act on the personal ID ("Official Gazette of RS", No. 24/2018).

[13] Legal Act on Cooperatives ("Official Gazette of RS" No. 122/2015).

[14] GDPR - General Data Protection Regulation.

[15] Commissioner for Information of Public Importance and Protection of Personal Data, Decision No. 164-00-00193/2011-07 dated September 29, 2011. year.

[16] Decision of the Appellate Court in Belgrade, No. 1360/2014 dated 05/21/2014. year.

[17] https://www.halpernadvisors.com/why-is-confidentiality-important/ (accessed on 04/24/2024. year).

[18] https://www.dsgvo-portal.de/gdpr-fines/gdpr-fine-against-bristol-logistics-sa-2023-01-12-RO-2499.php (accessed on September 1st, 2024.)

[19] https://vreme.com/nedelja/doktore-dajte-prst/ (accessed on September 1st, 2024.)